IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants:	Michael Roeder et al.	Examiner: Bryan F. Wright
Serial No.:	10/812,607	Group Art Unit: 2431
Filed:	March 30, 2004	Docket No.: 200313511-1
Due Date:	**February 16, 2010**	
Title:	SECURE INFORMATION DISTRIBUTION BETWEEN NODES (NETWORK DEVICES)	

APPEAL BRIEF UNDER 37 C.F.R. §41.37

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

This Appeal Brief is submitted in support of the Notice of Appeal filed on December 16, 2009, appealing the final rejection of claims 1-6, 10-30, 32, and 35-58 of the above-identified application as set forth in the Final Office Action mailed October 16, 2009.

The U.S. Patent and Trademark Office is hereby authorized to charge Deposit Account No. 08-2025 in the amount of $510.00 for filing a Brief in Support of an Appeal as set forth under 37 C.F.R. §41.20(b)(2). At any time during the pendency of this application, please charge any required fees or credit any overpayment to Deposit Account No. 08-2025.

Appellants respectfully request consideration and reversal of the Examiner's rejection of pending claims 1-6, 10-30, 32, and 35-58.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, LP having a principal place of business at 11445 Compaq Center Drive West, Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant that will have a bearing on the Board's decision in the present Appeal.

STATUS OF CLAIMS

In a Final Office Action mailed October 16, 2009, claims 1-6, 10-30, 32, and 35-58 were finally rejected. No claims have been withdrawn. No claims were objected to. Claims 7-9, 31, 33, and 34 have been canceled. Claims 1-6, 10-30, 32, and 35-58 are pending in the application. Claims 1-6, 10-30, 32, and 35-58 are the subject of the present Appeal.

STATUS OF AMENDMENTS

No amendments have been filed subsequent to the Final Office Action mailed October 16, 2009.

SUMMARY OF THE CLAIMED SUBJECT MATTER

The Summary is set forth as an exemplary embodiment as the language corresponding to independent claims 1, 25, 49, and 50. Discussions about elements of claims 1, 25, 49, and 50 can be found at least at the cited locations in the specification and drawings.

One aspect of the present invention, as claimed in independent claim 1, provides a method of secure information distribution between nodes (105). The method includes: providing, by a first node (105a), a component value A1; providing, by an adjacent node (105b), a component value B1 as a challenge to the first node; performing, by the first node, a handshake process with the adjacent node to determine membership in a secure group (160); wherein the handshake process comprises requiring each of the first node and the adjacent

node to calculate identical values by applying the component values A1 and B1, and a key value (167) associated with the secure group, to a one way function f(x); and distributing secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group. *See Specification*, page 13, line 5 through page 16, line 6; and Figure 1.

Another aspect of the present invention, as claimed in independent claim 25, provides an apparatus (100) for secure information distribution between nodes (105). The apparatus includes: a node (105a) configured to performing a handshake process with an adjacent node (105b) to determine membership in a secure group (160), and distribute secure information to the adjacent node, if the adjacent node is proven to be a member of the secure group; wherein the handshake process comprises requiring each of the node and the adjacent node to calculate identical values by applying a component value A1 provided by the node, a component value B1 provided by the adjacent node, and a key value (167) associated with the secure group, to a one way function f(x). *See Specification*, page 13, line 5 through page 16, line 6; and Figure 1.

Yet another aspect of the present invention, as claimed in independent claim 49, provides an apparatus (100) for secure information distribution between nodes (105). The apparatus includes: means for performing a handshake process between a first node (105a) and an adjacent node (105b) to determine membership in a secure group (160); wherein the handshake process comprises requiring each of the first node and the adjacent node to prove a key value (167) that is associated with the secure group; wherein each of the first node and the adjacent node has an identifier value (165) that is associated with the secure group in order for the first node and the adjacent node to calculate identical values by applying a component value A1 provided by the first node, a component value B1 provided by the adjacent node, and the key value associated with the secure group, to a one way function f(x); and means for distributing secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group. *See Specification*, page 13, line 5 through page 16, line 6; and Figure 1.

Yet another aspect of the present invention, as claimed in independent claim 50, provides an article of manufacture including a machine-readable medium having stored thereon instructions to: perform a handshake process between a first node (105a) and an

adjacent node (105b) to determine membership in a secure group (160); wherein the handshake process includes requiring each of the first node and the adjacent node to prove a key value (167) that is associated with the secure group; wherein each of the first node and the adjacent node has an identifier value (165) that is associated with the secure group in order for the first node and the adjacent node to calculate identical values by applying a component value A1 provided by the first node, a component value B1 provided by the adjacent node, and the key value associated with the secure group, to a one way function f(x); and distribute secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group. *See Specification*, page 13, line 5 through page 16, line 6; and Figure 1.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Whether claims 1-6, 10, 12, 16-19, 25-30, 32, 36, 40-43, and 49-58 are patentable under 35 U.S.C. § 103(a) over the combination of Krohn, U.S. Patent Publication No. 2004/0236965 ("Krohn") and Balfanz et al., U.S. Patent No. 7,392,387 ("Balfanz") in view of Dondeti et al., U.S. Patent No. 6,263,435 ("Dondeti") and further in view of Palekar et al., U.S. Patent Publication 2003/0226017 ("Palekar").

II. Whether claims 11, 13, 20, 21, 35, 37, 44, and 45 are patentable under 35 U.S.C. § 103(a) over the combination of Krohn, Balfanz, Dondeti, and Palekar, as applied to claims 1 and 25, and further in view of Benantar et al., U.S. Patent No. 6,854,056 ("Benantar").

III. Whether claims 14, 15, 23, 24, 38, 39, 47, and 48 are patentable under 35 U.S.C. § 103(a) over the combination of Krohn, Balfanz, Dondeti and Palekar, as applied to claims 1 and 25, and further in view of Hafer, U.S. Patent No. 4,530,092 ("Hafer").

IV. Whether claims 22 and 46 are patentable under 35 U.S.C. § 103(a) over the combination of Krohn, Balfanz, Dondeti and Palekar, as applied to claims 1 and 25, and further in view of Levine et al., U.S. Patent Publication No. 2003/0061481 ("Levine").

ARGUMENT

I. The Applicable Law

With regard to a 35 U.S.C. § 103 obviousness rejection: "Patent examiners carry the responsibility of making sure that the standard of patentability enunciated by the Supreme Court and by the Congress is applied in each and every case." M.P.E.P. 2141 (emphasis in the original). The Examiner bears the burden under 35 U.S.C. § 103 in establishing a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074 [5 USPQ2d 1596, 1598] (Fed. Cir. 1988).

One criteria that must be satisfied to establish a *prima facie* case of obviousness is the reference or combined references must teach or suggest all of the claim limitations. *In re Royka*, 490 F.2d 981 [180 USPQ 580] (C.C.P.A. 1974).

However, "[a] patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR Int'l Co. v. Teleflex, Inc.,* 127 S. Ct. 1727, 1731 [82 USPQ2d 1385, 1389] (2007). In making an obviousness determination over a combination of prior art references, it is "important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does." *Id. at* 1738 [1396].

To facilitate review of the determination of whether there was an apparent reason to combine known elements in the fashion claimed by the patent at issue, the "analysis should be made explicit." *Id. at* 1738 [1396]. "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988 [78 USPQ2d 1329] (Fed. Cir. 2006) (cited with approval in *KSR*, 127 S. Ct. at 1738 [82 USPQ2d at 1396]).

The test for obviousness under § 103 must take into consideration the invention as a whole; that is, one must consider the particular problem solved by the combination of elements that define the invention. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143 [227 USPQ 543, 551] (Fed. Cir. 1985). Furthermore, claims must be interpreted in light of the specification, claim language, other claims, and prosecution history. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1568 [1 USPQ2d 1593, 1597] (Fed. Cir. 1987), *cert. denied*, 481 U.S. 1052 (1987). At the same time, a prior patent cited as a § 103 reference

must be considered in its entirety, "*i.e.* as a *whole*, including portions that lead away from the invention." *Id.* That is, the Examiner must recognize and consider not only the similarities, but also the critical differences between the claimed invention and the prior art as one of the factual inquiries pertinent to any obviousness inquiry under 35 U.S.C. § 103. *In re Bond*, 910 F.2d 831, 834 [15 USPQ2d 1566, 1568] (Fed. Cir. 1990) (emphasis added).

Furthermore, the Examiner must avoid hindsight. *Id.* "A fact finder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning." *KSR,* 127 S. Ct. at 1739 [82 USPQ2d at 1397] (citing to *Graham v. John Deere*, 383 U.S. 1 [148 USPQ 459] (1966) in warning against a temptation to read into the prior art the teachings of the invention at issue and instructing courts to guard against slipping into the use of hindsight).

"[W]hen the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be nonobvious." *KSR,* 127 S. Ct. at 1737 [82 USPQ2d at 1395] (citing to *United States v. Adams*, 383 U.S. 39, 51-52 [148 USPQ 479] (1966).

In conclusion, an Appellant is entitled to a patent grant if a *prima facie* case of obviousness is not established. The Federal Circuit has endorsed this view in stating: "If examination at the initial stage does not produce a *prima facie* case of unpatentability, then without more the Appellant is entitled to grant of the patent." In re Oetiker, 977 F.2d 1443, 1446 [24 USPQ2d 1443, 1448] (Fed. Cir. 1992).

II. Rejection of claims 1-6, 10, 12, 16-19, 25-30, 32, 36, 40-43, and 49-58 as being unpatentable under 35 U.S.C. § 103(a) over the combination of Krohn, U.S. Patent Publication No. 2004/0236965 ("Krohn") and Balfanz et al., U.S. Patent No. 7,392,387 ("Balfanz") in view of Dondeti et al., U.S. Patent No. 6,263,435 ("Dondeti") and further in view of Palekar et al., U.S. Patent Publication 2003/0226017 ("Palekar").

The combination of Krohn, Balfanz, Dondeti, and Palekar fail to render claims 1-6, 10, 12, 16-19, 25-30, 32, 36, 40-43, and 49-58 *prima facie* obvious.

Appellants submit that Krohn, Balfanz, Dondeti, and Palekar, either alone, or in combination, fail to teach or suggest the limitations recited by independent claim 1 including "**wherein the handshake process comprises requiring each of the first node and the**

adjacent node to calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group, to a one way function f(x)."

The Examiner admits that Krohn in view of Balfanz and in further view of Dondeti, fails to disclose several features of independent claim 1, specifically, "providing, by a first node, a component value A1; providing, by an adjacent node, a component value B1 as a challenge to the first node;" and "wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group, to a one way function f(x)." (Final Office Action mailed October 16, 2009, pages 4-5). The Examiner, however, submits that these limitations are disclosed by Palekar. (Final Office Action mailed October 16, 2009, pages 5). Appellants respectfully disagree.

Palekar discloses an authentication procedure between an authenticator and a client. The procedure "begins with the authenticator sending the challenge (i.e., a component value) to the client." (Para. [0083]). Next, "the client then responds with a calculated value and a challenge of its own" noting that "***the calculated value could be a hash of the challenge and a password.***" (*Id,* emphasis added). Finally, "the authenticator calculates internally the value it expects from the client [and] compares those values" to determine if authentication is successful. (*Id*).

This procedure fails to disclose the features of independent claim 1. Indeed, as discussed above, independent claim 1 recites a handshake process whereby the first node and the adjacent node calculate values by ***applying three values to a one way function*** (e.g., a hash function). These three values include component value A1, component value B2, and a key value associated with the secure group. Palekar does not disclose applying such values to a one way function. Indeed, Palekar only discloses calculating a value by applying a single component value and a password to a hash function.

Notably, Palekar discloses that the protocol authentication procedure provides for the "use of additional inputs into the hash equation, as will be described in more detail below." (*Id*). The only other discussion in Palekar, however, with respect to the described authentication procedure discusses packet length attributes and these are not even discussed with respect to being inputs in the described hash function. (See Para. [0085]).

As such, while Palekar discloses two component values (one associated with the authenticator entity and one associated with the client entity), the one way function only takes as input ***a single component value***. As noted, Palekar discloses calculating a hash value using the challenge and a password as inputs. While the language of Palekar is ambiguous as to which challenge (i.e. component) value is being used, it is clear that only a single value is being used (by use of "***the*** challenge"). Further, there is no reference anywhere in Palekar to a key value associated with the secure group, let alone that value being included as an input along with the two component values into the one way function as recited in claim 1.

In addition, Appellants submit that it is improper to combine the cited references to make a rejection under 35 U.S.C. § 103(a). For example, consider the last step in claim 1 which recites "distributing secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group." This step contains a condition ("if the adjacent node is proven…") and an action ("distributing secure information…") to be performed if that condition is satisfied. The Examiner attempts to show this element is known in the prior art by citing one reference as disclosing the condition (Dondeti) and citing another as disclosing the action (Balfanz). (Final Office Action mailed October 16, 2009, pages 3-4). Such a rejection fails to acknowledge the inherent logical relationship between the two parts of an "if-then" statement. Appellants respectfully suggest that this rejection evidences "picking and choosing" features, taking them out of context and combining them when there is no suggestion in those references to do so.

In view of the above, Appellants submit that the above rejection of independent claim 1 under 35 U.S.C. § 103(a) should be withdrawn. Dependent claims 2-6, 10, 12, 16-19, 51, and 52 further define patentably distinct independent claim 1. Accordingly, Appellants believe that these dependent claims are also allowable over the cited references.

For similar reasons as discussed above with reference to independent claim 1, Appellants submit that Krohn, Balfanz, Dondeti, and Palekar, either alone, or in combination, also fail to teach or suggest the limitations recited by independent claim 25 including "**wherein the handshake process comprises requiring each of the node and the adjacent node to calculate identical values by applying a component value A1 provided by the node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group, to a one way function f(x);**" the limitations recited by

independent claim 49 including "**wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to calculate identical values by applying a component value A1 provided by the first node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group, to a one way function f(x)**;" and the limitations recited by independent claim 50 including "**calculate identical values by applying a component value A1 provided by the first node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group, to a one way function f(x)**."

In view of the above, Appellants submit that the above rejection of independent claims 25, 49, and 50 under 35 U.S.C. § 103(a) should be withdrawn. Dependent claims 26-30, 32, 36, 40-43, and 53-58 further define patentably distinct independent claim 25, 49, or 50. Accordingly, Appellants believe that these dependent claims are also allowable over the cited references.

Therefore, Appellants respectfully request reversal of the rejection of claims 1-6, 10, 12, 16-19, 25-30, 32, 36, 40-43, and 49-58 under 35 U.S.C. § 103(a).

III. Rejection of claims 11, 13, 20, 21, 35, 37, 44, and 45 as being unpatentable under 35 U.S.C. § 103(a) over the combination of Krohn, Balfanz, Dondeti, and Palekar, as applied to claims 1 and 25, and further in view of Benantar et al., U.S. Patent No. 6,854,056 ("Benantar").

The combination of Krohn, Balfanz, Dondeti, Palekar, and Benantar fail to render claims 11, 13, 20, 21, 35, 37, 44, and 45 *prima facie* obvious.

Dependent claims 11, 13, 20, 21, 35, 37, 44, and 45 further define patentably distinct independent claim 1 or 25. Accordingly, Appellants believe that these dependent claims are also allowable over the cited references.

In addition, the Examiner admits that Krohn, Balfanz, Dondeti, and Palekar fail to disclose the limitations recited by claims 11, 13, 20, 21, 35, 37, 44, and 45. (Final Office Action mailed October 16, 2009, pages 28 and 30). The Examiner submits that Benantar discloses these claim limitations. (Final Office Action mailed October 16, 2009, pages 28-31). Appellants respectfully disagree.

Benantar discloses a system for coupling identities through the use of digital certificates, thereby allowing a client to be authenticated for a variety of services without those services having to modify their existing methods of authentication. (Abstract).

Claims 11 and 35

Appellants submit that Krohn, Balfanz, Dondeti, Palekar, and Benantar, either alone, or in combination, fail to teach or suggest the limitations recited by dependent claims 11 and 35 including "**wherein the secure information comprises a password**."

The Examiner submits Benantar teaches this claim limitation at column 2, lines 9-12. (Final Office Action mailed October 16, 2009, page 29). Benantar merely discloses that most legacy systems ensure secure access through the use of a password or other secret or secure information, such as biometric identifiers, that must be simultaneously asserted along with a user's identity. (Col. 2, lines 9-12). Claims 11 and 35 recite that the secure information (i.e., a password) is distributed from the first node to the second node if the adjacent node is proven to be a member of the secure group. In contrast, the password disclosed by Benantar is used to obtain access to the system, the password is not distributed after the access to the system has already been obtained. Benantar does not disclose distributing a password from a first node to the adjacent node after secure access to the adjacent node from the first node is obtained.

In view of the above, Appellants respectfully request reversal of the rejection of claims 11 and 35 under 35 U.S.C. § 103(a).

Claims 13 and 37

Appellants submit that Krohn, Balfanz, Dondeti, Palekar, and Benantar, either alone, or in combination, fail to teach or suggest the limitations recited by dependent claim 13 including "**distributing secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information**;" and the limitations recited by dependent claim 37 including "**wherein the node is configured to distribute the secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information**."

The Examiner submits Benantar teaches these claim limitation at column 8, lines 60-67. (Final Office Action mailed October 16, 2009, page 29). Benantar merely discloses that a user 702 receives newly generated digital certificates 722, and user 702 may then publish

digital certificates 722 as necessary to engage in trusted transactions or trusted communications. An entity that receives digital certificate 722 may verify the signature of the CA by using CA public key 718, which is published and available to the verifying entity. (Col. 8, lines 62-67). Benantar does not disclose distributing an updated digital certificate to *each adjacent node that is a member of the secure group, in response to an update* of the digital certificate. Rather, in Benantar a user sends the digital certificate to a host system only when access to the host system is desired. (See col. 9, lines 1-15).

In view of the above, Appellants respectfully request reversal of the rejection of claims 13 and 37 under 35 U.S.C. § 103(a).

Claims 20 and 44

Appellants submit that Krohn, Balfanz, Dondeti, Palekar, and Benantar, either alone, or in combination, fail to teach or suggest the limitations recited by dependent claim 20 including "**resolving an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value**;" and the limitations recited by dependent claim 44 including **wherein the node is configured to resolve an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value**."

The Examiner submits Benantar teaches these claim limitations at column 6, lines 45-50. (Final Office Action mailed October 16, 2009, page 29). Benantar merely discloses that host system 310 receives authentication data 308, which can be reconciled with identity information in system registry 312, and host system 310 may then allow user 302 to use its services and resources. (Col. 6, lines 45-49). Benantar does not disclose resolving an ambiguity between received updated authentication data and currently stored authentication data by selecting the authentication data *with a larger data value*. Rather, Benantar is just disclosing that the received authentication data is verified by the host based on the identity information before allowing the user access to the host.

In view of the above, Appellants respectfully request reversal of the rejection of claims 20 and 44 under 35 U.S.C. § 103(a).

Claims 21 and 45

Appellants submit that Krohn, Balfanz, Dondeti, Palekar, and Benantar, either alone, or in combination, fail to teach or suggest the limitations recited by dependent claim 21 including "**increasing a security of the secure group by widening the key value which is known by each node in the secure group**;" and the limitations recited by dependent claim 45 including "**wherein the node is configured to increase a security of the secure group by widening the key value which is known by each node in the secure group**."

The Examiner submits Benantar teaches these claim limitations at column 4, lines 35-45. (Final Office Action mailed October 16, 2009, page 29). Benantar merely discloses that each party's public key is published while the private key is kept secret. Public keys are numbers associated with a particular entity and are intended to be known to everyone who needs to have trusted interactions with that entity. Private keys are numbers that are supposed to be known only to a particular entity, i.e., kept secret. In a typical public key cryptographic system, a private key corresponds to exactly one public key. (Col. 4, lines 35-43). Benantar does not disclose *increasing a security of a secure group by widening* the public or private key value which is known by each node in the secure group. Benantar only mentions public and private keys, not increasing the security of a secure group.

In view of the above, Appellants respectfully request reversal of the rejection of claims 21 and 45 under 35 U.S.C. § 103(a).

IV. Rejection of claims 14, 15, 23, 24, 38, 39, 47, and 48 as being unpatentable under 35 U.S.C. § 103(a) over the combination of Krohn, Balfanz, Dondeti and Palekar, as applied to claims 1 and 25, and further in view of Hafer, U.S. Patent No. 4,530,092 ("Hafer").

The combination of Krohn, Balfanz, Dondeti, Palekar, and Hafer fail to render claims 14, 15, 23, 24, 38, 39, 47, and 48 *prima facie* obvious.

Dependent claims 14, 15, 23, 24, 38, 39, 47, and 48 further define patentably distinct independent claim 1 or 25. Accordingly, Appellants believe that these dependent claims are also allowable over the cited references.

In addition, the Examiner admits that Krohn, Balfanz, Dondeti, and Palekar fail to disclose the limitations recited by claims 14, 15, 23, 24, 38, 39, 47, and 48. (Final Office

Action mailed October 16, 2009, pages 32-35). The Examiner submits that Hafer discloses these claim limitations. (Final Office Action mailed October 16, 2009, pages 32-35). Appellants respectfully disagree.

Hafer discloses a distributed switching system having multiple time slot interchanger nodes. Communications between stations served by different time slot interchangers (TSI) nodes in a telecommunications network are made possible without the use of either an intermediate stage of time multiplex space division switching or central time slot allocation by an arrangement in which each TSI node is linked to every other node by a patent in which each node time slots are "broadcast" to every other node in the network. (Abstract).

Hafer is in a different field of endeavor than Krohn, Balfanz, Dondeti, and Palekar. While Krohn, Balfanz, Dondeti, and Palekar relate to authentication for secure communications, Hafer relates to a distributed switching system having multiple time slot interchanger nodes. Hafer is not at all related to authentication. Therefore, one skilled in the art would not combine Hafer with Krohn, Balfanz, Dondeti, and Palekar and arrive at the limitations recited by claims 14, 15, 23, 24, 38, 39, 47, and 48. Further, Hafer fails to teach or suggest the limitations recited by claims 14, 15, 23, 24, 38, 39, 47, and 48 as discussed below.

Claims 14 and 38

Appellants submit that Krohn, Balfanz, Dondeti, Palekar, and Hafer, either alone, or in combination, fail to teach or suggest the limitations recited by dependent claim 14 including "**wherein the action of performing the handshake process comprises: performing the handshake process with the adjacent node once for every fixed time amount T**;" and the limitations recited by dependent claim 38 including "**wherein the node is configured to perform the handshake process with the adjacent node once for every fixed time amount T**."

The Examiner submits Hafer teaches these claim limitations at column 9, lines 40-45. (Final Office Action mailed October 16, 2009, page 33). Hafer merely discloses means operable when the observed broadcast time slot requests allocation of the time slot at the first node and the time slot is idle at the first node for broadcasting an acknowledgement signal. (Col. 9, lines 41-44). Hafer does not disclose a *handshake process*, let alone performing a handshake process with the adjacent node *once for every fixed time amount T*.

In view of the above, Appellants respectfully request reversal of the rejection of claims 14 and 38 under 35 U.S.C. § 103(a).

Claims 15 and 39

Appellants submit that Krohn, Balfanz, Dondeti, Palekar, and Hafer, either alone, or in combination, fail to teach or suggest the limitations recited by dependent claim 15 including "**after detecting the presence of another node that is not in an adjacency set, attempting to handshake with that another node if a detecting node and the another node both have a handshake time remaining value of zero (0)**;" and the limitations recited by dependent claim 39 including "**wherein the node is configured to attempt to handshake with another node if the node and the another node both have a handshake time remaining value of zero (0)**."

The Examiner submits Hafer teaches these claim limitations at column 9, lines 40-45. (Final Office Action mailed October 16, 2009, page 33). Hafer merely discloses means operable when the observed broadcast time slot requests allocation of the time slot at the first node and the time slot is idle at the first node for broadcasting an acknowledgement signal. (Col. 9, lines 41-44). Hafer does not disclose a *handshake process*, let alone *attempting to handshake with that another node if a detecting node and the another node both have a handshake time remaining value of zero (0)*.

In view of the above, Appellants respectfully request reversal of the rejection of claims 15 and 39 under 35 U.S.C. § 103(a).

Claims 23 and 47

Appellants submit that Krohn, Balfanz, Dondeti, Palekar, and Hafer, either alone, or in combination, fail to teach or suggest the limitations recited by dependent claim 23 including "**allowing for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes**;" and the limitations recited by dependent claim 47 including "**wherein the node is configured to allow for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes**."

The Examiner submits Hafer teaches these claim limitations at column 9, lines 40-45. (Final Office Action mailed October 16, 2009, page 33). Hafer merely discloses means operable when the observed broadcast time slot requests allocation of the time slot at the first node and the time slot is idle at the first node for broadcasting an acknowledgement signal. (Col. 9, lines 41-44). Hafer does not disclose a *handshake process*, let alone *allowing for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes*.

In view of the above, Appellants respectfully request reversal of the rejection of claims 23 and 47 under 35 U.S.C. § 103(a).

Claims 24 and 48

Appellants submit that Krohn, Balfanz, Dondeti, Palekar, and Hafer, either alone, or in combination, fail to teach or suggest the limitations recited by dependent claim 24 including "**preventing a single node in the secure group from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW $\pm$ TR between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range**;" and the limitations recited by dependent claim 48 including "**wherein the node is prevented from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW $\pm$ TR between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range**."

The Examiner submits Hafer teaches these claim limitations at column 9, lines 40-45 and at column 5, lines 19-27. (Final Office Action mailed October 16, 2009, pages 34 and 36). Hafer merely discloses means operable when the observed broadcast time slot requests allocation of the time slot at the first node and the time slot is idle at the first node for broadcasting an acknowledgement signal. (Col. 9, lines 41-44). Hafer also discloses that one simple technique is to distribute to all the elements of Figure 4 a common clock signal that signifies the beginning of each time slot period. The synchronization of time slot "j" incoming from the remote nodes over respective cables SC-2 through SC-m with the time slot

"j" of time slot interchanger 120 is achieved by equipping receivers 160 through 170 with buffers. (Col. 5, lines 19-26). Hafer does not disclose a *handshake process*, let alone *preventing a single node in the secure group from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW ± TR between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range.*

In view of the above, Appellants respectfully request reversal of the rejection of claims 24 and 48 under 35 U.S.C. § 103(a).

V. Rejection of claims 22 and 46 as being unpatentable under 35 U.S.C. § 103(a) over the combination of Krohn, Balfanz, Dondeti and Palekar, as applied to claims 1 and 25, and further in view of Levine et al., U.S. Patent Publication No. 2003/0061481 ("Levine").

The combination of Krohn, Balfanz, Dondeti, Palekar, and Levine fail to render claims 22 and 46 *prima facie* obvious.

Dependent claims 22 and 46 further define patentably distinct independent claim 1 or 25. Accordingly, Appellants believe that these dependent claims are also allowable over the cited references.

In addition, Appellants submit that Krohn, Balfanz, Dondeti, Palekar, and Levine, either alone, or in combination, fail to teach or suggest the limitations recited by dependent claim 22 including "**decreasing an amount of time between symmetric key regeneration (TK) to increase the security of the secure group**;" and the limitations recited by dependent claim 46 including "**wherein the node is configured to decrease an amount of time between symmetric key regeneration (TK) to increase the security of the secure group**."

The Examiner admits that Krohn, Balfanz, Dondeti, and Palekar fail to disclose the limitations recited by claims 22 and 46. (Final Office Action mailed October 16, 2009, page 37). The Examiner submits that Levine discloses these claim limitations. (Final Office Action mailed October 16, 2009, page 37). Appellants respectfully disagree.

Levine discloses a secure broadcast system having a plurality of nodes connected to a network with pre-positioned public/private encryption keys, including at least one root node

for publishing digital messages, a plurality of interior nodes for relaying the published digital messages, and a plurality of leaf nodes for receiving the published and relayed messages. Each digital message includes an encrypted payload, and a symmetric key for decrypting the payload. (Abstract).

The Examiner submits Levine teaches these claim limitations at paragraph 65, lines 1-16. (Final Office Action mailed October 16, 2009, page 37). Levine merely discloses that the payload is encrypted, and a new symmetric key is generated by the root node. This results in a set of encrypted symmetric keys, one for each of the direct recipient nodes of the root node. (Para. [0065]). Levine does not disclose *decreasing an amount of time between symmetric key regeneration to increase the security of* the root node and recipient nodes. Levine just discloses generating a symmetric key. (Para. [0065]).

In view of the above, Appellants respectfully request reversal of the rejection of claims 22 and 46 under 35 U.S.C. § 103(a).

CONCLUSION

For the above reasons, Appellants respectfully submit that the cited references neither anticipate nor render obvious the claims of the pending Application. The pending claims distinguish over the cited references, and therefore, Appellants respectfully submit that the rejections must be withdrawn, and respectfully request the Examiner be reversed and claims 1-6, 10-30, 32, and 35-58 be allowed.

Any inquiry regarding this Appeal Brief should be directed to Mark A. Peterson at Telephone No. (612) 573-0120, Facsimile No. (612) 573-2005.

Respectfully submitted,

Michael Roeder et al.,

By their attorneys,

DICKE, BILLIG & CZAJA, PLLC

Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2000
Facsimile: (612) 573-2005

Dated: February 16, 2010
MAP:cjs

/Mark A. Peterson/
Mark A. Peterson
Reg. No. 50,485

CLAIMS APPENDIX

1. (Previously Presented) A method of secure information distribution between nodes, the method comprising:

providing, by a first node, a component value A1;

providing, by an adjacent node, a component value B1 as a challenge to the first node;

performing, by the first node, a handshake process with the adjacent node to determine membership in a secure group;

wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group, to a one way function f(x); and

distributing secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group.

2. (Original) The method of claim 1, further comprising:

prior to providing the secure information to the adjacent node, performing the handshake process with another adjacent node.

3. (Original) The method of claim 1, further comprising:

establishing an encryption key with the adjacent node.

4. (Original) The method of claim 3, wherein the encryption key comprises a public key.

5. (Original) The method of claim 3, wherein the encryption key comprises a symmetric key.

6. (Original) The method of claim 3, wherein the secure information is distributed along with an encryption key.

7-9. (Cancelled)

10. (Previously Presented) The method of claim 1, wherein the one way function f(x) is a secure hash function.

11. (Original) The method of claim 1, wherein the secure information comprises a password.

12 (Original) The method of claim 1, wherein the secure information comprises a key for secure communication.

13. (Original) The method of claim 1, further comprising:

distributing secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information.

14. (Original) The method of claim 1, wherein the action of performing the handshake process comprises:

performing the handshake process with the adjacent node once for every fixed time amount T.

15. (Original) The method of claim 1, further comprising:

after detecting the presence of another node that is not in an adjacency set, attempting to handshake with that another node if a detecting node and the another node both have a handshake time remaining value of zero (0).

16. (Original) The method of claim 1, further comprising:

determining an age of the secure information so that each node in the secure group will store a latest version of the secure information.

17. (Original) The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking a sequence number of the secure information to determine the age of the secure information.

18. (Original) The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking a date of modification of the secure information to determine the age of the secure information.

19. (Original) The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking an elapsed time since a previous modification of the secure information to determine the age of the secure information.

20. (Original) The method of claim 1, further comprising:

resolving an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value.

21. (Previously Presented) The method of claim 1, further comprising:

increasing a security of the secure group by widening the key value which is known by each node in the secure group.

22. (Original) The method of claim 1, further comprising:

decreasing an amount of time between symmetric key regeneration (TK) to increase the security of the secure group.

23. (Original) The method of claim 1, further comprising:

allowing for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes.

24. (Original) The method of claim 1, further comprising:

preventing a single node in the secure group from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW $\pm$ TR between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range.

25. (Previously Presented) An apparatus for secure information distribution between nodes, the apparatus comprising:

a node configured to performing a handshake process with an adjacent node to determine membership in a secure group, and distribute secure information to the adjacent node, if the adjacent node is proven to be a member of the secure group;

wherein the handshake process comprises requiring each of the node and the adjacent node to calculate identical values by applying a component value A1 provided by the node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group, to a one way function f(x).

26. (Original) The apparatus of claim 25, wherein the node performs the handshake process with another adjacent node, prior to providing the secure information to the adjacent node.

27. (Original) The apparatus of claim 25, wherein the node is configured to establish an encryption key with the adjacent node.

28. (Original) The apparatus of claim 25, wherein the encryption key comprises a public key.

29. (Original) The apparatus of claim 25, wherein the encryption key comprises a symmetric key.

30. (Original) The apparatus of claim 27, wherein the secure information is distributed along with an encryption key.

31. (Cancelled)

32. (Previously Presented) The apparatus of claim 25, wherein the one way function f(x) is a secure hash function.

33-34. (Cancelled)

35. (Original) The apparatus of claim 25, wherein the secure information comprises a password.

36. (Original) The apparatus of claim 25, wherein the secure information comprises a key for secure communication.

37. (Original) The apparatus of claim 25, wherein the node is configured to distribute the secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information.

38. (Original) The apparatus of claim 25, wherein the node is configured to perform the handshake process with the adjacent node once for every fixed time amount T.

39. (Original) The apparatus of claim 25, wherein the node is configured to attempt to handshake with another node if the node and the another node both have a handshake time remaining value of zero (0).

40. (Original) The apparatus of claim 25, wherein the node is configured to determine an age of the secure information so that each node in the secure group will store a latest version of the secure information.

41. (Original) The apparatus of claim 25, wherein the node is configured to check a sequence number of the secure information to determine the age of the secure information.

42. (Original) The apparatus of claim 25, wherein the node is configured to check a date of modification of the secure information to determine the age of the secure information.

43. (Original) The apparatus of claim 25, wherein the node is configured to check an elapsed time since a previous modification of the secure information to determine the age of the secure information.

44. (Original) The apparatus of claim 25, wherein the node is configured to resolve an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value.

45. (Previously Presented) The apparatus of claim 25, wherein the node is configured to increase a security of the secure group by widening the key value which is known by each node in the secure group.

46. (Original) The apparatus of claim 25, wherein the node is configured to decrease an amount of time between symmetric key regeneration (TK) to increase the security of the secure group.

47. (Original) The apparatus of claim 25, wherein the node is configured to allow for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes.

48. (Original) The apparatus of claim 25, wherein the node is prevented from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW $\pm$ TR between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range.

49. (Currently Amended) An apparatus for secure information distribution between nodes, the apparatus comprising:

means for performing a handshake process between a first node and an adjacent node to determine membership in a secure group;

wherein the handshake process comprises requiring each of the first node and the adjacent node to prove a key value that is associated with the secure group;

wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to calculate identical values by applying a component value A1 provided by the first node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group, to a one way function f(x); and

means for distributing secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group.

50. (Previously Presented) An article of manufacture, comprising:

a machine-readable medium having stored thereon instructions to:

perform a handshake process between a first node and an adjacent node to determine membership in a secure group;

wherein the handshake process comprises requiring each of the first node and the adjacent node to prove a key value that is associated with the secure group;

wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to

calculate identical values by applying a component value A1 provided by the first node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group, to a one way function f(x); and

distribute secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group.

51. (Previously Presented) The method of claim 1, wherein the handshake process further comprises:

transmitting the calculated value between the first node and the adjacent node.

52. (Previously Presented) The method of claim 1,

wherein the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.

53. (Previously Presented) The apparatus of claim 25, wherein the handshake process further comprises:

transmitting the calculated value between the node and the adjacent node.

54. (Previously Presented) The apparatus of claim 25,

wherein the node belongs to the secure group if the node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.

55. (Previously Presented) The apparatus of claim 49, wherein the handshake process further comprises:

transmitting the calculated value between the first node and the adjacent node.

56. (Previously Presented) The apparatus of claim 49,

wherein the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.

57. (Previously Presented) The article of manufacture of claim 50, wherein the handshake process further comprises:

transmitting the calculated value between the first node and the adjacent node.

58. (Previously Presented) The article of manufacture of claim 50,

wherein the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.